UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/783,617	02/20/2004	Tom Kenney	NC34726	7222

7590 11/04/2005

Tom Weber
c/o Nokia Mobile Phones (Patent Dept.)
Mail Stop 1-4-755
6000 Connection Drive
Irving, TX 75039

EXAMINER	
FOX, BRYAN J	

ART UNIT	PAPER NUMBER
2686	

DATE MAILED: 11/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/783,617	KENNEY, TOM	
	Examiner	Art Unit	
	Bryan J. Fox	2686	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 6, 7, 9, 12-15, 18-20, 22-24 and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Muthuswamy et al (US 20040137893A1).

Regarding **claim 1**, Muthuswamy et al disclose a system where a user reports his communication device as stolen by calling the service provider or carrier operating the communication system. Once the device is reported stolen, access to the communication system by the communication device is locked (i.e. disabled), and the memory is erased (see paragraph 37 and figure 4), which reads on the claimed, "system that limits mobile device functionality via a wireless network, comprising: an input component that receives a remotely originated request to disable the mobile device; and a disabling component that limits access to memory within the mobile device based on the request."

Regarding **claim 2**, Muthuswamy et al disclose that the communication device includes the security application 165 that processes security messages received and can be programmed into the communication device. The security application initiates

the complete erasure of the information memory (see paragraphs 31-32), which reads on the claimed, "the request activates a pre-programmed security feature stored within the mobile device."

Regarding **claim 3**, Muthuswamy et al disclose that once the device is reported stolen, the memory can be erased (see paragraph 37 and figure 4), which reads on the claimed, "the security feature erases data stored in the mobile device's memory."

Regarding **claim 6**, Muthuswamy et al disclose that the invention can be a wireless communication system or the communication system could use Bluetooth, among other protocols (see paragraph 17), which reads on the claimed, "the wireless network protocol is one of an IS2000, a CDMA, a TCDMA, a WCDMA, a TDMA, a FDMA, a GSM, a PCS, a Bluetooth, a Wi-Fi, a Cellular and a GPS protocol."

Regarding **claim 7**, Muthuswamy et al disclose that the communication network sends a message to the device to disable it (see paragraph 37), which reads on the claimed, "the request is broadcast to the mobile device via one of a one-time transmission, a periodic transmission and a continuous transmission."

Regarding **claim 9**, Muthuswamy et al disclose that the device is locked, the memory is erased, and optionally, hardware can be disabled (see paragraph 37 and figure 4), which reads on the claimed, "the disabling component further limits mobile device access via at least one of a keypad lock, a voice lock, a screen blank-out and a deletion of the device memory."

Regarding **claim 12**, Muthuswamy et al disclose that the information is transferred form the stolen device to the backup server (see paragraph 37 and figure 4),

which reads on the claimed, "the request further invokes remote storage of the data stored within the mobile device's memory."

Regarding **claim 13**, Muthuswamy et al disclose that the user can call the service provider or the carrier operating the communication system to report that the communication device is stolen (see paragraph 37), which reads on the claimed, "a signal outside the wireless network is utilized to send the request to disable the mobile device's memory," wherein the phone call may be outside the wireless network.

Regarding **claim 14**, Muthuswamy et al disclose that the communication device can be a mobile cellular telephone, a personal digital assistant or a laptop computer among other electronic devices (see paragraph 18), which reads on the claimed, "the system of claim 1 is employed in one of a laptop computer, a handheld computer, a notebook computer, a personal digital assistant, a mobile telephone and a desktop computer."

Regarding **claim 15**, Muthuswamy et al disclose a system where a user reports his communication device as stolen by calling the service provider or carrier operating the communication system. Once the device is reported stolen, access to the communication system by the communication device is locked (i.e. disabled), and the memory is erased (see paragraph 37 and figure 4), which reads on the claimed, "method that limits access to a mobile device utilizing a wireless network, comprising: receiving a request to disable the mobile device; broadcasting a disable signal to the mobile device; and disabling access to at least the mobile device memory."

Regarding **claim 18**, Muthuswamy et al disclose that the invention can be a wireless communication system or the communication system could use Bluetooth, among other protocols (see paragraph 17), which reads on the claimed, "broadcasting the signal via at least one of an IS2000, a CDMA, a TCDMA, a WCDMA, a TDMA, a FDMA, a GSM, a PCS, a Bluetooth, a Wi-Fi, a Cellular and a GPS protocol."

Regarding **claim 19**, Muthuswamy et al disclose that the communication device includes the security application 165 that processes security messages received and can be programmed into the communication device. The security application initiates the complete erasure of the information memory (see paragraphs 31-32), which reads on the claimed, "access is disabled via at least one of the mobile device's internal security features."

Regarding **claim 20**, Muthuswamy et al disclose that the device is locked, the memory is erased, and optionally, hardware can be disabled (see paragraph 37 and figure 4), which reads on the claimed, "disabling access to the device comprises one or more of blanking a screen, locking a keypad, locking a microphone, and deleting mobile device memory."

Regarding **claim 22**, Muthuswamy et al disclose that the communication device can be a mobile cellular telephone, a personal digital assistant or a laptop computer among other electronic devices (see paragraph 18), which reads on the claimed, "the method of claim 15 is employed in connection with at least one of a laptop computer, a handheld computer, a notebook computer, a personal digital assistant, a mobile telephone and a desktop computer."

Regarding **claim 23**, Muthuswamy et al disclose that the user can call the service provider or the carrier operating the communication system to report that the communication device is stolen (see paragraph 37), which reads on the claimed, "the disable signal is sent via a third-party network," wherein the phone call may be outside the wireless network.

Regarding **claim 24**, Muthuswamy et al disclose a system where a user reports his communication device as stolen by calling the service provider or carrier operating the communication system. Once the device is reported stolen, access to the communication system by the communication device is locked (i.e. disabled), and the memory is erased (see paragraph 37 and figure 4), which reads on the claimed, "method that disables functionality of a mobile device via a wireless network, comprising: receiving a disable signal from a remote location; extracting information from the disable signal; and disabling memory access of mobile device based on the extracted information."

Regarding **claim 26**, Muthuswamy et al disclose that the operations are performed via security notifications (see paragraph 32), which reads on the claimed, "the signal is embedded in the wireless network's signaling protocol."

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 4, 8, 16, 21, 25 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muthuswamy et al in view of Hayatake et al (US005734978A).

Regarding **claim 4**, Muthuswamy et al disclose the request may be transmitted via a phone call (see paragraph 37). Muthuswamy et al fail to expressly disclose it is verified based on a caller identification.

In a similar field of endeavor, Hayatake et al disclose a system where a unique cryptographic number is used that only the user knows (see column 4, lines 12-24), which reads on the claimed, "a caller identification."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Hayatake et al to include the above use of a unique cryptographic number that only the user knows in order to prevent unauthorized people from locking the users computer.

Regarding **claim 8**, Muthuswamy et al fail to disclose a return signal to verify access to the mobile device memory has been limited.

In a similar field of endeavor, Hayatake et al disclose a system where after destroying the data in the phone, the control section transmits a destruction end signal

to the telephone informing the user of the destruction (see column 5, lines 5-15 and figure 2B).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Hayatake et al to include the above destruction confirmation signal so that the legal owner of the stolen mobile telephone can confirm that the mobile telephone has been made unavailable as suggested by Hayatake et al (see column 5, lines 5-15).

Regarding **claim 16**, Muthuswamy et al fail to expressly disclose authenticating the request with a mobile device owner.

In a similar field of endeavor, Hayatake et al disclose that to prevent illegal use, a user as a legal owner of the mobile telephone needs to input a string of arbitrary numerical digits which only the user knows to destroy the data of the mobile telephone (see column 4, lines 12-24), which reads on the claimed, "authenticating the request with a mobile device owner."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Hayatake et al to include the above use of a cryptographic number in order to ensure that only the owner of the device can initiate the destruction of the data.

Regarding **claim 21**, Muthuswamy et al fails to expressly disclose that the request to disable access to the device is transmitted upon an unauthorized use.

In a similar field of endeavor, Hayatake et al disclose a system where the request to disable the phone is repeated, and can only function when the cell phone is turned on

and is registered (see column 6, line 66 – column 7, line 23), which reads on the claimed, "the request to disable access to the device is transmitted upon an unauthorized use," wherein turning the stolen cell phone on reads on unauthorized use.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Hayatake et al to include the above transmission of the request when the cell phone is on in order to ensure that the request is received.

Regarding **claim 25**, Muthuswamy et al fail to disclose a return signal that indicates the functionality of the device has been disabled.

In a similar field of endeavor, Hayatake et al disclose a system where after destroying the data in the phone, the control section transmits a destruction end signal to the telephone informing the user of the destruction (see column 5, lines 5-15 and figure 2B).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Hayatake et al to include the above destruction confirmation signal so that the legal owner of the stolen mobile telephone can confirm that the mobile telephone has been made unavailable as suggested by Hayatake et al (see column 5, lines 5-15).

Regarding **claim 27**, Muthuswamy et al disclose a system where a user reports his communication device as stolen by calling the service provider or carrier operating the communication system. Once the device is reported stolen, access to the communication system by the communication device is locked (i.e. disabled), and the

memory is erased (see paragraph 37 and figure 4), which reads on the claimed, "system that facilitates limiting device functionality, comprising: means for receiving a signal to disable device functionality; means for limiting device functionality based on the signal." Muthuswamy et al fail to disclose means for transmitting a return signal indicating successful disabling of device functionality.

In a similar field of endeavor, Hayatake et al disclose a system where after destroying the data in the phone, the control section transmits a destruction end signal to the telephone informing the user of the destruction (see column 5, lines 5-15 and figure 2B).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Hayatake et al to include the above destruction confirmation signal so that the legal owner of the stolen mobile telephone can confirm that the mobile telephone has been made unavailable as suggested by Hayatake et al (see column 5, lines 5-15).

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Muthuswamy et al in view of Cocita (US 20040204021A1).

Regarding **claim 5**, Muthuswamy et al fails to expressly disclose that the request to disable the mobile device is made by placing a wireless phone call that invokes the request.

In a similar field of endeavor, Cocita discloses that if the cell phone is stolen or lost, the user may, using another cell phone or a land line, request the data to be erased

(see paragraph 23), which reads on the claimed, "the request to disable the mobile device is made by placing a wireless phone call that invokes the request."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Cocita to include the above request via a cell phone in order to provide maximum convenience to the user.

Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muthuswamy et al in view of Trommelen (US006813487B1).

Regarding **claim 10**, Muthuswamy et al fail to disclose a tracking component that utilizes the request to facilitate locating the mobile device.

In a similar field of endeavor, Trommelen discloses a system that determines a geographic location of a lost or stolen mobile device (see column 3, line 63 – column 4, line 24 and figure 3), which reads on the claimed, "tracking component that utilizes the request to facilitate locating the mobile device."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Trommelen to include the above locating the lost or stolen mobile device in order to assist in device recovery as suggested by Trommelen (see column 4, lines 25-54).

Regarding **claim 11**, Muthuswamy et al fail to disclose the tracking component employs one or more of a global positioning system, a homing beacon and an audio alarm.

In a similar field of endeavor, Trommelen discloses the locating system may employ a GPS receiver (see column 3, line 63 – column 4, line 24), which reads on the claimed, "the tracking component employs one or more of a global positioning system, a homing beacon and an audio alarm."

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Trommelen to include the above GPS receiver in order to take advantage of a very accurate positioning system already in place.

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Muthuswamy et al in view of Isikoff (US005748084A).

Regarding **claim 17**, Muthuswamy et al fail to disclose locating the mobile device after the disable signal has been sent.

In a similar field of endeavor, Isikoff discloses a system where when a computer is stolen, data on the laptop is destroyed, and finally, the signals transmitted by the cellular transceiver are externally tracked to determine the location of the computer (see column 8, line 22 – column 9, line 52).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Muthuswamy et al with Isikoff to include the above locating the computer after destroying the data in order to assist in the recovery of the computer hardware as suggested by Isikoff (see column 9, lines 33-52).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Pagliaroli et al (US005276728A) disclose a remotely activated automobile disabling system.

Tiedemann, Jr. et al (US006546243B2) disclose a method and system for over-the-air service programming.

Singhal (US 20040203595A1) discloses a method and apparatus for user authentication using a cellular telephone and a transient pass code.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bryan J. Fox whose telephone number is (571) 272-7908. The examiner can normally be reached on Monday through Friday 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Marsha Banks-Harold can be reached on (571) 272-7905. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Bryan Fox
November 2, 2005

CHARLES APPIAH
PRIMARY EXAMINER